Document made available under the Patent Cooperation Treaty (PCT)

International application number: PCT/JP05/003967

International filing date: 08 March 2005 (08.03.2005)

Document type: Certified copy of priority document

Document details: Country/Office: JP
Number: 2004-067004
Filing date: 10 March 2004 (10.03.2004)

Date of receipt at the International Bureau: 12 May 2005 (12.05.2005)

Remark: Priority document submitted or transmitted to the International Bureau in compliance with Rule 17.1(a) or (b)

PCT/JP2005/003967

10.3.2005

日本国特許庁
JAPAN PATENT OFFICE

別紙添付の書類に記載されている事項は下記の出願書類に記載されている事項と同一であることを証明する。

This is to certify that the annexed is a true copy of the following application as filed with this Office.

出願年月日 Date of Application:	２００４年　３月１０日
出願番号 Application Number:	特願２００４－０６７００４
パリ条約による外国への出願に用いる優先権の主張の基礎となる出願の国コードと出願番号 The country code and number of your priority application, to be used for filing abroad under the Paris Convention, is	ＪＰ２００４－０６７００４
出願人 Applicant(s):	松下電器産業株式会社

２００５年　４月２０日

特許庁長官
Commissioner,
Japan Patent Office

小川洋

出証番号　出証特２００５－３０３６０４３

【書類名】　特許願
【整理番号】　2048260029
【提出日】　平成16年 3月10日
【あて先】　特許庁長官殿
【国際特許分類】　H04L 12/28
【発明者】
　【住所又は居所】　大阪府門真市大字門真１００６番地　松下電器産業株式会社内
　【氏名】　ライクセンリング　ジェルマーノ
【発明者】
　【住所又は居所】　大阪府門真市大字門真１００６番地　松下電器産業株式会社内
　【氏名】　金丸　智一
【発明者】
　【住所又は居所】　大阪府門真市大字門真１００６番地　松下電器産業株式会社内
　【氏名】　大薗　雅弘
【特許出願人】
　【識別番号】　000005821
　【氏名又は名称】　松下電器産業株式会社
【代理人】
　【識別番号】　100097445
　【弁理士】
　【氏名又は名称】　岩橋　文雄
【選任した代理人】
　【識別番号】　100103355
　【弁理士】
　【氏名又は名称】　坂口　智康
【選任した代理人】
　【識別番号】　100109667
　【弁理士】
　【氏名又は名称】　内藤　浩樹
【手数料の表示】
　【予納台帳番号】　011305
　【納付金額】　21,000円
【提出物件の目録】
　【物件名】　特許請求の範囲　1
　【物件名】　明細書　1
　【物件名】　図面　1
　【物件名】　要約書　1
　【包括委任状番号】　9809938

【書類名】特許請求の範囲
【請求項１】
リソース利用装置からリソース提供装置へのアクセスを制御するアクセス制御装置であって、
　リソース利用装置からリソース提供装置へのリソース利用を許可するアクセス制御をリソース提供装置に対して行うアクセス許可部と、
　アクセス制御装置とリソース利用装置との通信状態を監視する存在確認部と、
　存在確認部にてリソース利用装置とのリンク切断が確認された場合、前記アクセス制御を破棄する破棄制御をリソース提供装置に対して行うアクセス破棄部と、
　を備えたアクセス制御装置。
【請求項２】
上記アクセス許可部にてアクセス制御を行ったリソース利用装置とリソース提供装置との組を管理する許可情報管理手段を備え、
　上記存在確認部は、許可情報管理手段にて管理しているリソース利用装置のみとの通信状態を監視することを特徴とする請求項１記載のアクセス制御装置。
【請求項３】
アクセス制御を行ったリソース提供装置のうち、破棄制御を行う必要のあるひとつ以上のリソース提供装置を管理する破棄対象管理手段を備え、
　上記存在確認部は、リソース提供装置に対する特定のリソース利用装置のみとの通信状態を監視することを特徴とする請求項２記載のアクセス制御装置。
【請求項４】
アクセス制御装置よりアクセス制御され、リソース利用装置よりリソース利用されるリソース提供装置であって、
　リソース利用装置からのリソース利用を許可するアクセス許可部と、
　上記リソース提供装置とアクセス制御装置との通信状態を監視する存在確認部と、
　存在確認部にてアクセス制御装置とのリンク切断が確認された場合、前記アクセス制御を破棄するアクセス破棄部と、
　を備えたリソース提供装置。

【書類名】明細書
【発明の名称】リソース提供装置およびアクセス制御装置
【技術分野】
【０００１】
本発明は、電子機器のアクセス制御に関する。
【背景技術】
【０００２】
近年、電子機器のマルチユーザ化が進められ、同じ機器でも同時に複数のユーザが使うことが可能になった。ユーザが自身の機器を他人に貸しながら同時に機器を利用することができるようになった。
【０００３】
ネットワークを介してユーザが機器を貸し出す場合、セキュリティが最も重要な要素である。物理的な世界であればユーザが自身の手でものを渡し、誰がリソース利用をしているかを管理することができる。しかしネットワークを通した場合、知らない間に自身の機器が不正に他人に使われる恐れがある。
【０００４】
非特許文献１はその課題を解決するプロトコルである（以下、「ＵＰｎＰセキュリティ」とする）。ＵＰｎＰセキュリティを使うことで、ネットワークを介して電子機器のリソース利用のアクセス制御を行うことができる。リソース利用を制御する機器が、リソースを提供する機器へのアクセス制御命令をネットワーク上通信するための汎用的なプロトコルである。
【０００５】
また、ＵＰｎＰセキュリティでは、アクセス制御を行うときに破棄の条件を設定することができる。具体的に、アクセス制御に対して有効期間を設定することができる。
【０００６】
しかしながら、ＵＰｎＰセキュリティではアクセス制御を与えるときに有効期間がわからない場合は有効ではない。
【０００７】
つまりアクセス制御の破棄に関しては速やかに破棄するという技術が十分でない。アクセス制御の破棄は、実世界で破棄すべき状態になってから実際に破棄されるまでの間を限りなく０に近づけなければならない。
【０００８】
また、特許文献１では無線通信機能を備えた複数の機器における使用許可を制御する技術が公開されている。特許文献１で定義されている機器グループにおいて、使用許可装置とグループ内のひとつの機器の存在確認ができなくなるとすべての機器を使用不許可にすることができる。
【特許文献１】特開２００３－２８９３０７号公報
【非特許文献１】UPnP Device Security and Security Console V, UPnP Forum, 2003, http://www.upnp.org/standardizeddcps/security.asp
【発明の開示】
【発明が解決しようとする課題】
【０００９】
しかしながら、特開２００３－２８９３０７号公報ではアクセス制御される電子機器をユーザ同士が共有することができないという課題を有していた。
【００１０】
本発明は、前記従来の課題を解決するもので、破棄すべきアクセス制御を速やかに破棄し、リソースを提供する機器の不正な使用を防止することを目的とする。
【課題を解決するための手段】
【００１１】
前期従来の課題を解決するために、第１の発明によれば、アクセス制御装置は、リソー

ス利用装置からリソース提供装置へのアクセスを許可するアクセス制御を行い、アクセス許可装置とリソース利用装置との通信状態を監視し、リソース利用装置とのリンク切断が確認された場合、前期アクセス制御を破棄する破棄制御をリソース提供装置に対して行うことによって、リソース提供装置の不正な使用を防止することができる。

【００１２】

また、アクセス制御装置は、アクセス制御を行ったリソース利用装置とリソース提供装置との組を管理し、管理しているリソース利用装置のみとの通信状態を監視するようにしてもよい。

【００１３】

また、アクセス制御装置は、アクセス制御を行ったリソース提供装置のうち、破棄制御を行う必要のあるひとつ以上のリソース提供装置を管理し、リソース提供装置を利用する特定のリソース利用装置のみとの通信状態を監視するようにしてもよい。

【００１４】

本発明の第２の発明によれば、リソース提供装置は、アクセス制御装置よりアクセス制御され、リソース利用装置よりリソース利用され、リソース利用装置からのアクセスを許可し、リソース提供装置とアクセス制御装置との通信状態を監視し、存在確認部にてアクセス制御装置とのリンク切断が確認された場合、前期アクセス制御を破棄することによって、リソース提供装置の不正な使用を防止することができる。

【発明の効果】

【００１５】

本発明によれば、破棄すべきアクセス制御を速やかに破棄し、リソースを提供する機器の不正な使用を防止するリソース提供装置２０およびアクセス制御装置１０を提供することができる。

【発明を実施するための最良の形態】

【００１６】

以下、本発明の実施の形態について、図を用いて説明する。

【００１７】

（実施の形態１）

図１は、本発明の実施形態に係るアクセス制御システムの全体構成の一例を示す図である。図１において、アクセス制御システムは３つの電子機器１０、２０、３０と、それぞれの電子機器をつなぐ接続４０、５０、６０とを備える。アクセス制御装置１０は、リソース提供装置２０との接続４０上で通信を行い、リソース提供装置２０上に存在するリソースへのアクセスを制御する。リソース利用装置３０はリソース提供装置２０との接続５０上で通信を行い、リソース提供装置２０のリソースを利用する。アクセス制御装置１０はリソース利用装置３０との接続６０上で通信を行い、リソース利用装置３０の存在確認を行う。存在確認を行うことで、アクセス制御を速やかに破棄できる。

【００１８】

接続４０、５０、６０はインターネットなどのネットワークを介した接続や無線通信を使った接続や有線通信を使った接続などを指す。

【００１９】

リソース利用とは具体的にリソース提供装置２０に対して、記憶データへのアクセスやリソース提供装置２０が構成されるデバイスへの入出力などリソース提供装置２０の本来の機能を利用しリソース利用装置３０に有益な通信を指す。

【００２０】

このアクセス制御システムを利用する主な目的はリソース利用装置３０からリソース提供装置２０への通信を行いリソース利用をすることである。そのリソース利用はアクセス制御装置１０の制御のもとで行われる。図２はアクセス制御装置１０がアクセス制御を行うシーケンスの一例を示している。

【００２１】

リソース利用を制御できるため、アクセス制御装置１０とアクセス提供装置は事前準備

を行う必要がある。具体的にリソース提供装置２０は、アクセスができる機器としてアクセス制御装置１０を認めている必要がある。その方法は公知のものであり、具体的には非特許文献１の方法を採用できる。図２では、事前準備がすでに行われていて、リソース提供装置２０がアクセス制御装置１０からの命令を認証していて許可があると認めている。

【００２２】

アクセス制御装置１０がアクセス制御を行う場合、アクセス制御装置１０がリソース提供装置２０に対してアクセス制御命令を送信する（ステップＳ１）。また、アクセス制御装置１０がリソース利用装置３０に対してアクセス許可通知命令を送信する（ステップＳ２）。ステップＳ１とステップＳ２の順番はこだわらないが、次のステップＳ３を行うためにステップＳ１とステップＳ２が完了している必要がある。

【００２３】

尚、ステップＳ２ではアクセス制御装置１０がリソース利用装置３０に対してアクセス許可通知を行っているが、実装によってはステップＳ２の代替としてリソース提供装置２０がリソース利用装置３０に通知することも考えられる。あるいはユーザによる手動入力も可能である。重要なのはリソース利用装置３０にリソース利用が許可されたことを通知することである。

【００２４】

アクセス制御装置１０はアクセス制御命令を送信した後リソース利用装置３０の存在確認を行う（ステップＳ３）。ステップＳ３では存在確認が成功しているため、アクセス制御装置１０はアクセス制御の破棄を行わない。

【００２５】

ステップＳ１とステップＳ２が行われた後、リソース利用装置３０がリソース提供装置２０に対してアクセス制御が必要なリソースへのアクセス命令を送信できる（ステップＳ３）。リソース提供装置２０はアクセス命令を受信し、アクセス命令のアクセス許可を確認する。許可が認められた場合だけ、アクセス命令に応じてリソース利用が成功する。

【００２６】

アクセス制御装置１０はアクセス制御を送信した後リソース利用装置３０の存在確認を行い続ける（ステップＳ５）。ステップＳ５では存在確認に失敗しているため、アクセス制御装置１０がアクセス制御の破棄をしなければならないと判断する。

【００２７】

存在確認に失敗したため、アクセス制御装置１０がリソース提供装置２０に対してアクセス制御破棄命令を送信する（ステップＳ６）。リソース提供装置２０は、アクセス許可破棄命令を処理した後、ステップＳ４で行われていたアクセス命令に対して応じなくなりリソース利用が失敗する。

【００２８】

リソース利用が失敗した場合、リソース提供装置２０がリソース利用装置３０に対して失敗の理由を示すエラーコードを送信してもよい。

【００２９】

図３ではアクセス制御命令とアクセス制御通知命令とアクセス制御破棄命令に使われる構造体の一例を示す。構造体は、タイプと機器ＩＤとひとつ以上の許可情報を持つ。タイプとは、アクセス制御命令かアクセス制御通知命令かアクセス制御破棄命令かを特定する定数である。機器ＩＤとは具体的に機器のＩＰアドレスや、機器の公開鍵のハッシュ値や、機器の公開鍵など機器を特定できるＩＤを指す。制御情報とは、アクセス制御されるコマンド名の名前とコマンドに対するゼロ以上のパラメータ制限からなる。

【００３０】

尚、実施によってはアクセス制御命令やアクセス制御通知命令やアクセス制御破棄命令に許可情報を添付しない方法が考えられる。それはたとえば制御される命令やパラメータがシステム設計時に決定される場合が考えられる。

【００３１】

尚、上記構造体は一例であり、それぞれの命令が上記構造体に従わなくてもよい。たと

えば、アクセス制御装置１０とリソース提供装置２０の間であらかじめ決められた整理番号を利用し、アクセス制御破棄命令の中身はその整理番号だけで決められるようにしてもよい。そのとき、リソース提供装置２０は、受信した整理番号に基づいてどのアクセス制御を破棄すべきかを決定する。

【００３２】

図４ではアクセス制御装置１０がアクセス制御を行うための動作手順をフローチャートの形式で示している。

【００３３】

まずアクセス制御装置１０はリソース提供装置２０に対してアクセス制御命令を送信する（ステップＳ１０）。そしてアクセス制御装置１０はリソース利用装置３０に対してアクセス制御通知命令を送信する（ステップＳ１１）。アクセス許可通知を送信した後、アクセス制御装置１０がリソース利用装置３０の存在確認を行い（ステップＳ１２）、存在が確認できたかどうかの判断を行う（ステップＳ１３）。存在確認ができた場合、一定時間スリープを行う（ステップＳ１４）。一定時間スリープした後、存在確認を繰り返す。また、存在確認ができなかったと判断した場合、アクセス制御装置１０はリソース提供装置２０に対してアクセス破棄命令を送信しアクセス許可を破棄する（ステップＳ１５）。

【００３４】

アクセス制御装置１０が複数の機器を同時に監視できるため、許可情報管理テーブルが必要になる。図５ではアクセス制御装置１０が利用する許可情報管理テーブルの一例を示す。

【００３５】

提供側の列１００は、リソースを提供する特定のリソース提供装置２０との接続の情報が書き込まれる。アクセス制御破棄命令を配信するときに利用する接続である。

【００３６】

利用側の列１０１は、リソースを利用する特定のリソース利用装置３０との接続の情報が書き込まれる。存在確認を行うときに利用する接続である。

【００３７】

通信インターフェースの列１０２は、リソース利用装置３０の存在確認に利用されるひとつ以上のデバイスと通信プロトコルに依存した通信に関する制限を書き込むことができる。たとえば、ＩＰネットワークで通信を行う場合２点の通信において距離をＨＯＰという論理単位で計算することができるので１ＨＯＰ以内などと制限できる。

【００３８】

アクセスの列１０３は、破棄制御対象の制御情報が書き込まれる。

【００３９】

上記許可情報管理テーブルに基づいたアクセス制御装置１０は次の処理を行う。アクセス許可を与えたとき、許可情報管理テーブルに一行を追加する。定期的に許可情報管理テーブルの各行に基づいて存在確認を行い、存在確認ができなかった場合アクセス破棄命令を送信し対象の行を削除する。

【００４０】

上記許可情報管理テーブルを使った場合の存在確認およびアクセス制御破棄命令の送信は具体的に次のように行われる。通信インターフェースの列１０２に書いてある通信インターフェースを利用し、利用側の列１０１に書いてある機器の存在確認を順番に行う。存在確認ができなかった列に対してアクセス破棄命令の送信を行う。具体的に提供側の列１００に書いてあるリソース提供装置２０に対して利用側の列１０１に書いてあるリソース利用装置３０によるアクセスの列１０３に書いてあるリソース利用のアクセス制御破棄命令を送信する。そして存在確認ができなかった行を削除する。

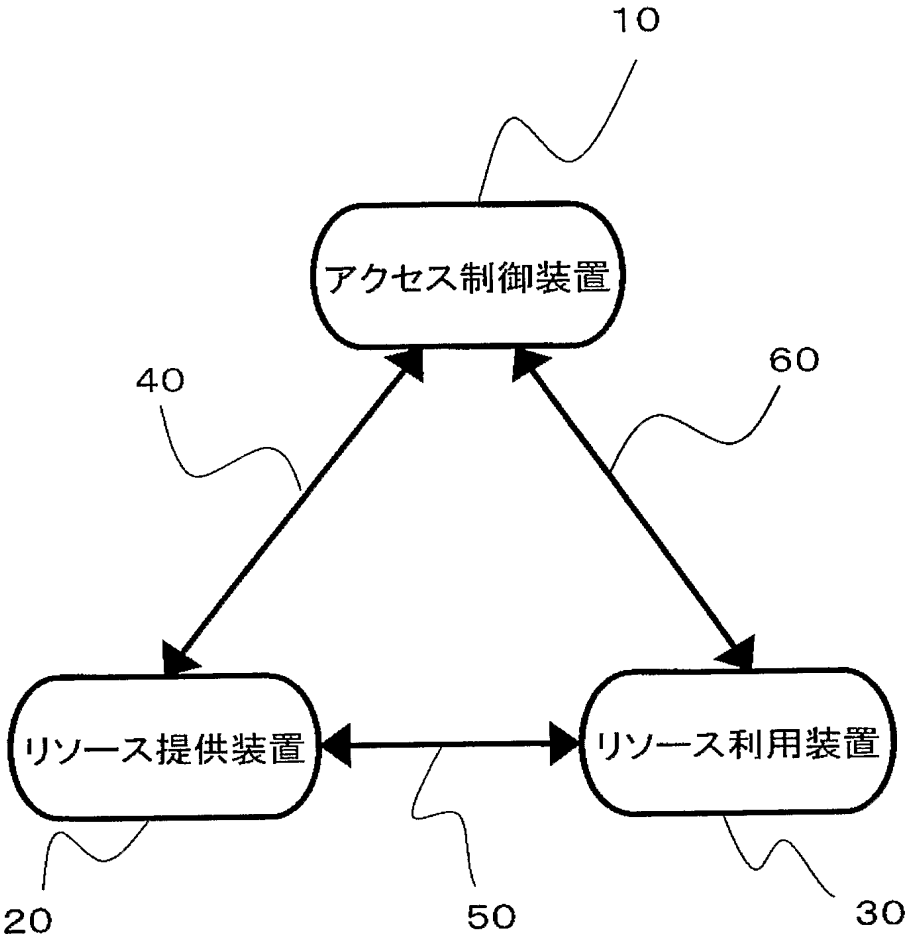
【００４１】

図５の２行目の例では、アクセス制御装置１０は通信インターフェースｅｔｈ０を利用し、携帯電話Ｅの存在確認を行う。そして携帯電話Ｅの存在確認ができなかった場合、携帯電話Ｂに対して携帯電話Ｅによる秘密資料参照のアクセス制御破棄命令を送信する。

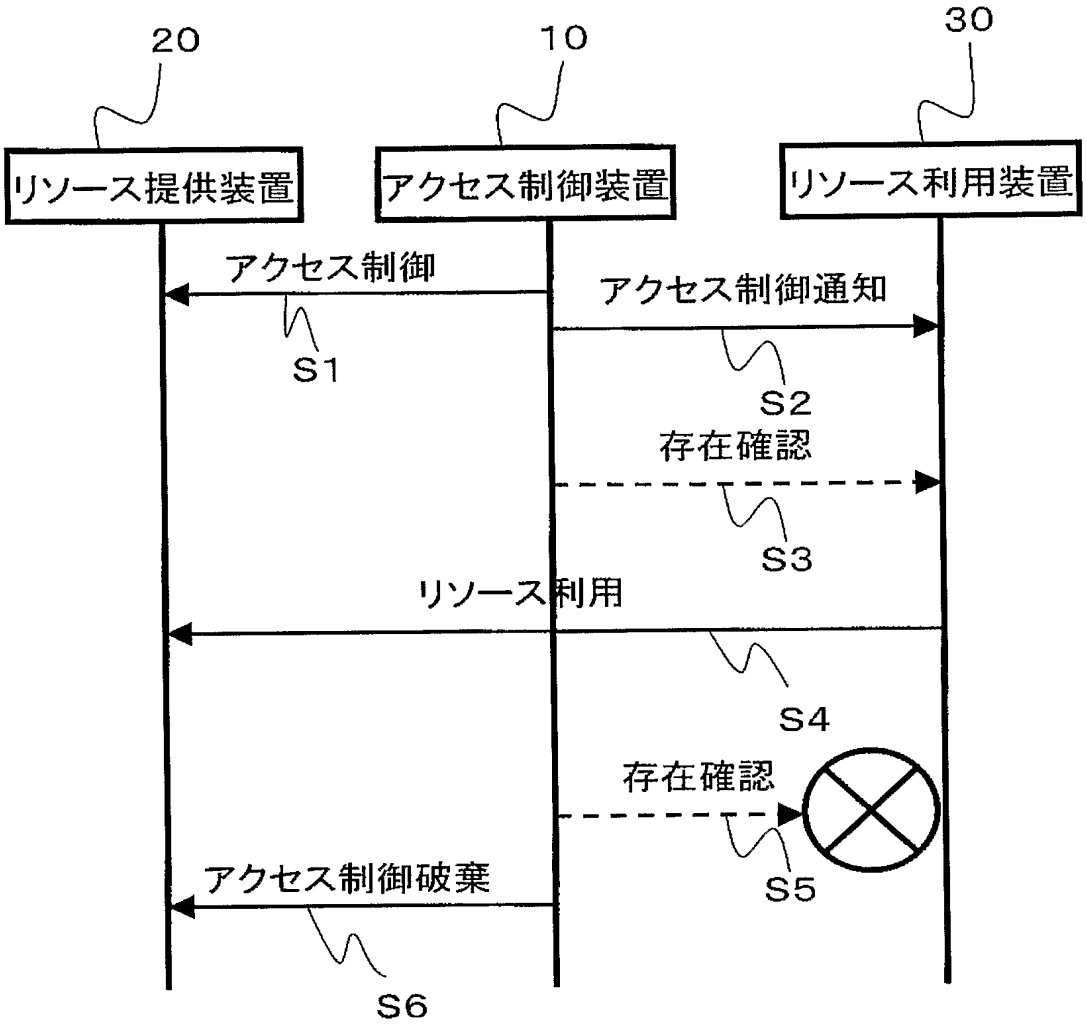
【００４２】
図５の３行目の例では、アクセス制御装置１０はすべての通信インターフェースを利用し、携帯電話Ｂの存在確認を行う。そしてどの通信インターフェースで存在確認を行っても携帯電話Ｂの存在確認ができなかった場合、据置機器Ｃに対して携帯電話Ｂによるビデオ視聴のアクセス制御破棄命令を送信する。
【００４３】
ただし、リソース提供装置２０とアクセス制御装置１０との間の通信が途絶された場合、アクセス制御装置１０がリソース提供装置２０に対してアクセス制御破棄命令を送信できなくなる。その場合はセキュリティの観点ではリソース提供装置２０側でアクセス制御を破棄する必要がある。
【００４４】
図６ではリソース提供装置２０の動作手順をフローチャートの形式で示している。
【００４５】
まずリソース提供装置２０はアクセス制御装置１０よりアクセス許可命令を受信し、アクセス管理テーブルを変更する（ステップＳ２０）。アクセス許可命令を受信した後、アクセス制御装置１０の存在確認をし続ける。具体的にアクセス制御装置１０の存在確認を行い（ステップＳ２１）、存在確認ができたかどうかの判断を行う（ステップＳ２２）。存在確認ができた場合、一定時間スリープを行う（ステップＳ２３）。一定時間スリープした後、存在確認を繰り返す。また、存在確認ができなかったと判断した場合、アクセス管理テーブルを変更しアクセス制御を破棄する（ステップＳ２４）。
【００４６】
リソース提供装置２０が複数の機器を同時に監視できるため、許可情報管理テーブルが必要になる。図７ではリソース提供装置２０が利用する許可情報管理テーブルの一例を示す。
【００４７】
制御側の列２００は、アクセス制御を行う特定のアクセス制御装置１０との接続情報が書き込まれる。存在確認を行うときに利用する接続である。
【００４８】
アクセスの列２０１は、破棄制御対象の制御情報が書き込まれる。
【００４９】
上記許可情報管理テーブルを使った場合の存在確認およびアクセス制御の破棄は次のように行われる。制御側の列２００に書いてある機器の存在確認を順番に行う。存在確認ができなかった行に対してアクセスの列２０１に書いてあるアクセス制御の破棄を行い、存在確認ができなかった行を削除する。
【００５０】
図７の２行目の例では、リソース提供装置２０は携帯電話Ｈの存在確認を行う。そして携帯電話Ｈの存在確認ができなかった場合、秘密資料参照のアクセス制御を破棄する。
【産業上の利用可能性】
【００５１】
電子機器のアクセス制御に関して、破棄すべきアクセス制御を速やかに破棄し、リソースを提供する機器の不正な使用を防止することに利用可能である。
【図面の簡単な説明】
【００５２】
【図１】本発明の実施形態に係るアクセス制御システムの全体構成の一例を示した図
【図２】アクセス制御装置１０がアクセス制御を行うシーケンスの一例を示した図
【図３】アクセス制御命令とアクセス制御通知命令とアクセス制御破棄命令に使われる構造体の一例を示した図
【図４】アクセス制御装置１０がアクセス制御を行うための動作手順のフローチャート
【図５】アクセス制御装置１０が利用する許可情報管理テーブルの一例を示した図

【図６】リソース提供装置の動作手順を示す図
【図７】リソース提供装置が利用する許可情報管理テーブルを示す図
【符号の説明】
【００５３】
１０　アクセス制御装置
２０　リソース提供装置
３０　リソース利用装置
４０　アクセス制御装置１０とリソース提供装置２０との接続
５０　リソース利用装置３０とリソース提供装置２０との接続
６０　アクセス制御装置１０とリソース利用装置３０との接続
１００　提供側の列
１０１　利用側の列
１０２　通信インターフェースの列
１０３　アクセスの列
２００　制御側の列
２０１　アクセスの列

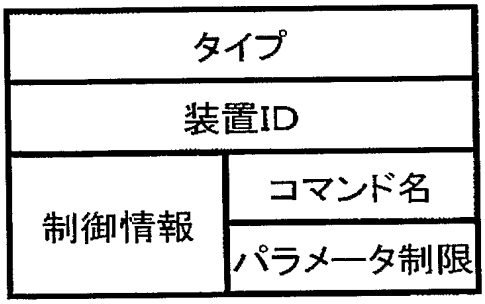
【書類名】図面
【図１】



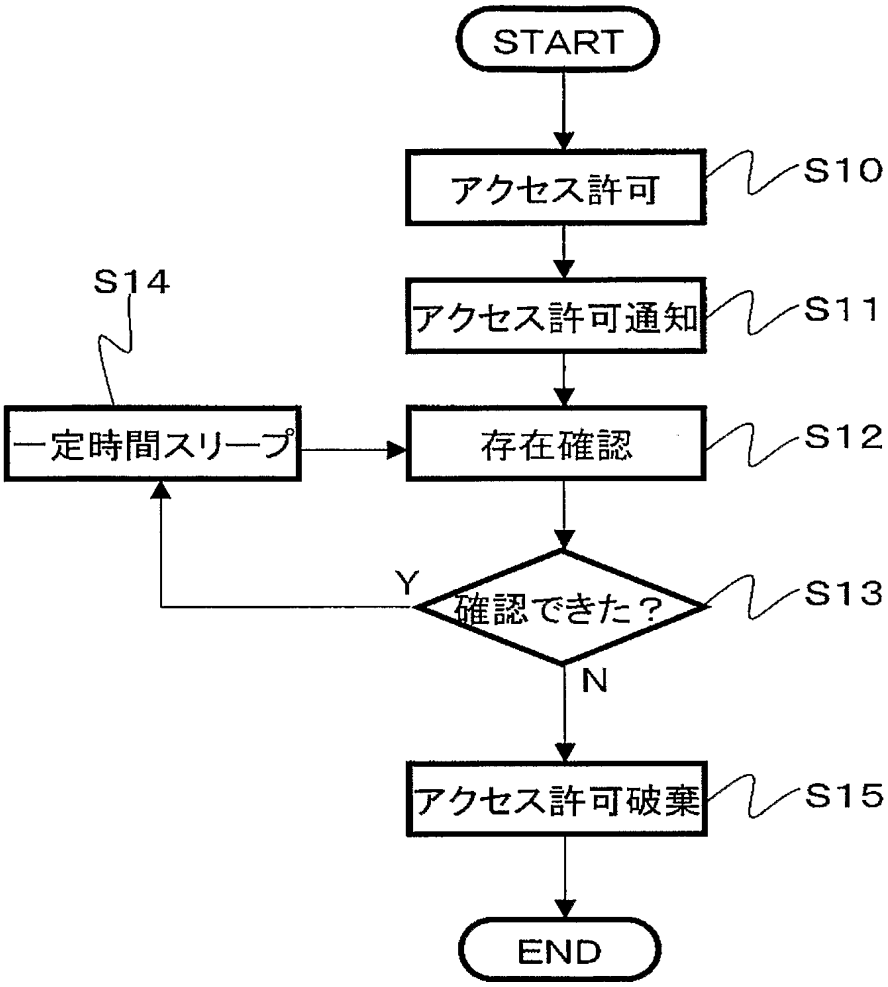
【図２】


20
10
30
リソース提供装置
アクセス制御装置
リソース利用装置
アクセス制御
S1
アクセス制御通知
S2
存在確認
S3
リソース利用
S4
存在確認
S5
アクセス制御破棄
S6

【図３】


タイプ
装置ID
制御情報
コマンド名
パラメータ制限

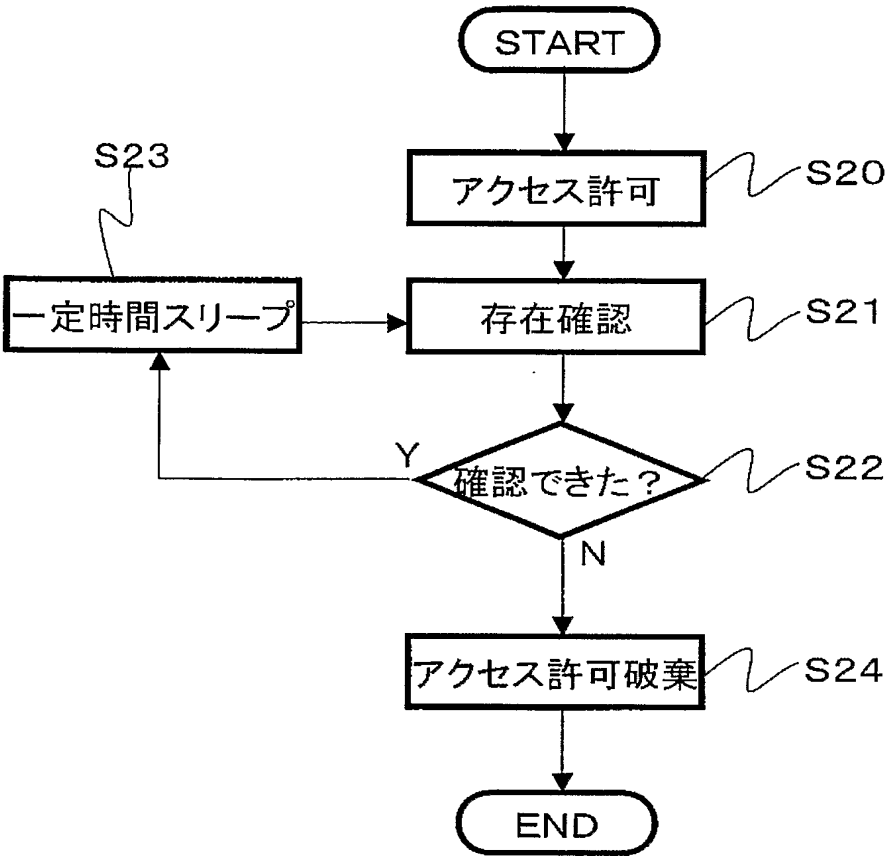
【図４】



【図５】

100 提供側	101 利用側	102 通信I/F	103 アクセス
携帯電話B	携帯電話E	eth0	秘密資料参照
据置機器C	携帯電話B	ANY	ビデオ視聴
パソコンD	携帯電話E	eth1	印刷
据置機器C	据置機器F	ttyS0	リモコン制御
パソコンD	パソコンG	eth0	ファイル書込み

【図６】



【図７】

200　　201

制御側	アクセス
携帯電話H	秘密資料参照
携帯電話H	ビデオ視聴
据置機器I	印刷
据置機器I	リモコン制御
パソコンJ	ファイル書込み

【書類名】要約書
【要約】
【課題】リソース提供装置２０の不正利用を防止する。
【解決手段】アクセス制御装置１０は、リソース利用装置３０からリソース提供装置２０へのアクセスを許可するアクセス制御を行い、アクセス許可装置とリソース利用装置３０との通信状態を監視し、リソース利用装置３０とのリンク切断が確認された場合、前期アクセス制御を破棄する破棄制御をリソース提供装置２０に対して行うことによって、リソース提供装置２０の不正な使用を防止することができる。
【選択図】図１

特願２００４－０６７００４

出　願　人　履　歴　情　報

識別番号　［０００００５８２１］

１．変更年月日　１９９０年　８月２８日
［変更理由］　新規登録
住　所　大阪府門真市大字門真１００６番地
氏　名　松下電器産業株式会社